

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with the six Google accounts
listed in Attachment A-2 that is stored at premises
controlled by Google LLC

Case No. 3:22-mj-379

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-2

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-2

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

SEE ATTACHMENT C-2

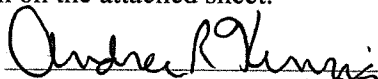
Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Andrea R. Kinzig, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone (specify reliable electronic means).

Date: 11/9/22

City and state: Dayton, OH


Peter B. Silvain, Jr.
United States Magistrate Judge



ATTACHMENT A-2
Property to Be Searched

Information associated with the Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com, kinstonmcgeorge6@gmail.com, kinstonmcgeorge80@gmail.com, kinstonmcgeorge45@gmail.com, kinstonmcgeorge9000@gmail.com, and kinstonmcgeorge7@gmail.com** that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B-2
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2 for the time period of January 1, 2021 to the present:

1. Subscriber Information: Any available subscriber information for the account, including the following: user-provided name; account email address; account status; Google services used by account; recovery email and SMS recovery number; account creation date and time; terms of service IP address, date, and time; language; Google Account ID ; last logins to the account, including IP address, date, and time; and accounts associated with a particular device, SMS recovery number, IMEI, or Android ID.
2. IP Logs: Logs of IP addresses utilized to access the Google account.
3. Gmail: The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.
4. Contacts: Any records pertaining to the user’s contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.
5. Calendar: Any records pertaining to the user’s calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history.
6. Messaging: The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
7. Google Drive and Google Keep: The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data

and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

8. Photos: The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
9. Maps: All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.
10. Location History: All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
11. Chrome and My Activity: All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyn Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any Internet or search history indicative of searching for child pornography or content involving children.
5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
6. Any communications with minors, and any identifying information for these minors.
7. Any information related to the use of aliases.
8. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
9. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
10. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
11. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
12. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-2

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI, New Paris (Ohio) Police Department, and Preble County (Ohio) Sheriff's Department, I am currently involved in an investigation of child pornography offenses committed by KINSTON MCGEORGE (hereinafter referred to as "MCGEORGE"). This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Information associated with the email accounts **kinstonmcgeorge@yahoo.com**, **kinstonmcgeorge69@yahoo.com**, and **kinstonmcgeorge80@yahoo.com** that is stored at premises controlled by Yahoo Inc. (as more fully described in Attachment A-1);
 - b. Information associated with the Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com**, **kinstonmcgeorge6@gmail.com**, **kinstonmcgeorge80@gmail.com**, **kinstonmcgeorge45@gmail.com**, **kinstonmcgeorge9000@gmail.com**, and **kinstonmcgeorge7@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-2);
 - c. Information associated with the Snapchat accounts containing the user names **dakingcobra69**, **kingcobraka2022**, and **dakingcobrakai7** and the user identification number of **a325813c-31ac-4553-897e-7d3ca0c2f4b0** that is stored at premises controlled by Snap Inc. (as more fully described in Attachment A-3);
 - d. Information associated with the Reddit accounts containing the user names **KingCobraKai7**, **Outside-Difference66**, **Cultural_Yogurt_6309**, **Ok-Rooster5362**, **Fun_Management2465**, and **Prudent_Economy8810** that is stored at premises controlled by Reddit Inc. (as more fully described in Attachment A-4);

- e. Information associated with the Discord accounts containing the user names **KingCobraKai69#6844** and **DatKingCobraKai420#4263** and the user identification numbers **586587119187918849** and **802267151120465970** that is stored at premises controlled by Discord Inc. (as more fully described in Attachment A-5);
 - f. Information associated with the Instagram account containing the user name **kinstonmegeorge** and the user identification number **54284524983** that is stored at premises controlled by Meta Platforms Inc. (as more fully described in Attachment A-6); and
 - g. Information associated with the Twitter account containing the user name **@KingCobraKai69** that is stored at premises controlled by Twitter Inc. (as more fully described in Attachment A-7).
3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:
- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2), which make it a crime to possess child pornography; and
 - b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.
4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-7 hereto and are incorporated by reference.
5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the above noted accounts (as defined in Attachments A-1 through A-7). It does not contain every fact known to the investigation.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1), are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-7).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. §§ 2252(a)(2) and (b)(1) state that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) state that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
12. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce

by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 through B-7 to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
 - e. **“Child erotica”**, as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
 - f. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a

fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- g. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- h. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- i. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- j. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

- k. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

Email Accounts

14. Yahoo Inc. is a company based in California. In my training and experience, I have learned that Yahoo Inc. provides a variety of online services, including electronic mail (“email”) access, to the public.
15. Yahoo Inc. allows subscribers to obtain email accounts at the domain name yahoo.com and ymail.com, like the account listed in Attachment A-1. Subscribers obtain accounts by registering with Yahoo Inc. During the registration process, Yahoo Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo Inc. subscribers) and information concerning subscribers and their use of Yahoo Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.
16. In general, emails that are sent to Yahoo Inc. subscribers are stored in the subscriber’s “mail box” on Yahoo Inc.’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the messages can remain on Yahoo Inc.’s servers indefinitely. Even if the subscriber deletes an email, it may continue to be available on Yahoo Inc.’s servers for a certain period of time.
17. Yahoo Inc. subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and

my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

19. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
20. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
21. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense

under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Google Services

22. Google LLC ("Google") is a multi-national corporation with its headquarters located in Mountain View, California. Google offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.
23. In addition, Google offers an operating system ("OS") for mobile devices (including cellular phones) known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.
24. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in user name for access to the Google Account. However, users can also sign up for Google accounts with third-party email addresses.
25. Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below. Google's services include but are not limited to the following:
 - a. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

- b. Contacts: Google provides address books for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.
- c. Calendar: Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.
- d. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.
- e. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made

changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me”. Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

- f. Google Keep: Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google’s cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.
- g. Google Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.
- h. Google Maps: Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.
- i. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the

inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

- j. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.
 - k. Android Backup: Android device users can use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, call history, contacts, device settings, or SMS messages. Users can also opt-in through Google One to back up photos, videos, and multimedia sent using Messages
26. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.
27. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

28. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.
29. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.
30. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.
31. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.
32. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).
34. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.
35. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Snapchat Accounts

36. Snapchat is a social media communication application owned by Snap Inc., a company based in Santa Monica, California. The application is available on cellular telephones and tablets. The application provides a means to send and receive "self-destructing" messages, pictures, and videos.
37. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed, it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaves the Chat screen, messages viewed by both the sender and receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and "snaps" constitute "electronic communications" within the meaning of 18 U.S.C. § 3123. See 18 U.S.C. §§ 3127(1) and 2510(12).
38. A user can type messages and send photos, videos, audio notes, and video notes to friends within the Snapchat application using the "Chat" feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the Chat by tapping on the message that he or she wants to keep. The user can clear the message by tapping it again.

39. “Our Stories” is a collection of user-submitted “Snaps” from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at an event could all contribute to the same “Our Stories” collection by sharing their snaps, even if they do not know each other. Users can also view “Our Stories” events if they are not actually present at the event by subscribing to the story.
40. In addition to “Our Stories”, a Snapchat user can keep a sort of photo / video diary using the “Story” feature. Each snap in a “Story” documents the user’s experience. Based on the user’s privacy settings, the photos and videos added to a “Story” can be viewed either by everyone on Snapchat or just the user’s friend. Stories are visible to other users for up to 24 hours.
41. “Snapcash” is an online money transfer service offered by Snapchat. The actual business platform is run by “SquareUp”, the distributor of a mobile credit card reader and application Square Register. Snapcash can be used to transfer money between Snapchat users using a linked, U.S.-issued Visa or MasterCard debit card only. Snapcash can only be sent to other users who have a linked debit card. Snapcash has a \$250 weekly limit but can be upgraded to a \$2,500 weekly limit. Users who upgrade have to provide their full name, date of birth, and Social Security Number.
42. Snapchat has a “Group Stories” feature that allows multiple users to contribute photos and videos to the same “Story”, a collection of posts that stays viewable for a limited amount of times. Snapchat users can name their group story and invite other users and “friends” by user name to add content. The Group Stories will disappear if 24 hours pass without a user adding a new photo or video.
43. “Memories” is a cloud-storage service provided by Snapchat. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone’s photo gallery in Snapchat’s Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.
44. Snapchat asks users to provide basic contact and personal identifying information when registering their accounts, to include date of birth. When a user creates an account, he/she creates a unique Snapchat user name. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account, and a new user must also provide a mobile telephone number. This telephone number is verified during the registration process. Snapchat sends an activation code to the telephone number that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a telephone number, so one may not always be present in the user’s account. Snapchat also retains the account creation date.

45. While a Snapchat message may disappear, the record of who sent it and when it was sent still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.
46. Snapchat stores device information such as the model, operating system, operating system version, mobile device telephone number, and mobile network information of devices used in conjunction with the service. Snapchat also collects unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event that the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.
47. If a user consents, Snapchat can access his/her device's electronic phone book or contacts list and images.
48. Snapchat retains information about the method and source of payment of customers who use the Snapcash service. This includes debit card information such as the card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and Social Security Number of those involved in money transfers. Snapcash generates a receipt for any transactions. The receipts are programmed to automatically delete after the sender and recipient have seen the message and swiped out of the Chat screen, unless either taps to save the message. Snapchat maintains transactional records for ten days. These records include information about the sender and receiver, the transaction amount, and the date/time stamps of when the message was sent, received, and opened.
49. Snapchat deletes a snap once it had been viewed. If the message is not read because the user has not opened up the application, the message is stored for 30 days before being deleted. However, just because the snap no longer appears to the user does not necessarily mean they are gone. For example, Snapchat has a feature called Replay. This allows users to view a previously viewed snap once per day. This feature is disabled by default and the user must opt-in to use Replay. Also, if a Snapchat user posts an image or video to the MyStory feature, it can be viewed by their friends for 24 hours. If the users posts to the Our Stories feature, the snaps are archived and can be viewed through Snapchat.
50. Therefore, the computers of Snap Inc. are likely to contain the material described above, including stored electronic communications and information concerning subscribers and

their use of Snapchat (such as account access information, transaction information, and account application).

Instagram

51. Instagram operates a photo and video sharing networking service located at <http://www.instagram.com>. As noted above, Instagram is owned by Meta Platforms Inc., formerly known as Facebook Inc.
52. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application (“app”) created by the company that allows users to access the service through a mobile device.
53. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various “tags” that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of “filters” or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also “like” photos.
54. Upon creating an Instagram account, an Instagram user must create a unique Instagram user name and an account password. This information is collected and maintained by Instagram.
55. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user’s full name, email addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.
56. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.
57. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block the, which prevents the blocked user from following that user.

58. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.
59. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.
60. Users on Instagram may also search Instagram for other users or particular types of photos or other content.
61. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP") address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.
62. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.
63. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.
64. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.
65. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.
66. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Instagram “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Discord

67. Discord is a messaging platform owned by Discord Inc. (“Discord”), a company based in San Francisco, California. Based on my training and experience, I have learned that Discord is a proprietary freeware instant messaging and VoIP application and digital distribution platform designed for creating communities ranging from gamers to education and businesses. Discord specializes in text, image, video and audio communication between users in chat channels. Discord runs on Windows, macOS Android, iOS, Linux, and in web browsers. As of July 21, 2019, there were over 250 million users of the software.
68. Discord uses the metaphors of servers and channels similar to Internet Relay Chat, although these servers do not map to traditional hardware or virtual servers due to its distributed nature. A user can create a server on Discord, manage its public visibility and access, and create one or more channels within this service. Within a server, depending on access controls, users can create channels within a category framework, with the visibility and access on the channels also customizable to the server. One such customization is the ability to mark channels “NSFW” (Not Safe For Work), which forces first-time channel viewers to confirm that they are over 18 and willing to see such content. In addition to normal text-based channels, Discord servers can create voice-chat channels.
69. Every Discord user has a unique four-digit “discriminator”, shown as a four-digit number, prefixed with “#”, after their username. This allows for multiple users to have the same username and for users to find friends easily.

70. Both at the server and the user level, Discord allows users to connect to their Twitch or other gaming service accounts. These integrations provide unique messaging tools within the application. For example, Discord can determine the game a user is presently playing on Steam if they have connected their account. Discord is specifically designed for use while gaming, as it includes features such as low-latency, free voice chat servers for users, and dedicated server infrastructure. Discord's developers also added video calling and screen sharing features in 2017. Support for calls between two or more users was added in an update on July 28, 2016.
71. While the software itself comes at no cost, the developers investigated ways to monetize it, with potential options including paid customization options such as emoji or stickers. In January 2017, the first paid subscription and features were released with "Discord Nitro Classic" (originally released as "Discord Nitro"). For a monthly subscription fee of \$4.99, users can get an animated avatar, use custom and/or animated emojis across all servers (non-nitro users can only use custom emoji on the server they were added to), an increased maximum file size on file uploads (from 8 MB to 50 MB), the ability to screen share in higher resolutions, and the ability to choose their own discriminator (from #0001 to #9999) and a unique profile badge. In October 2018, "Discord Nitro" was renamed "Discord Nitro Classic" with the introduction of the new "Discord Nitro", which cost \$9.99 and included access to free games through the Discord game store.
72. Video calling and screen sharing features were added to Discord, first for a small test base in August 2017 and later for all users in October 2017. While these features mimic live-streaming capabilities of platforms like Twitch, the company does not plan to compete with these services, believing that these features are best used by small groups.
73. Based on its online law enforcement guide, I know that Discord maintains the following information for its accounts:
 - a. The unique user ID number of the account that is assigned by Discord;
 - b. Registration date and time for the account;
 - c. Registration IP address of the account;
 - d. Email address provided by the user;
 - e. User's current username and tag number;
 - f. Billing information for paid subscribers;

- g. IP addresses and session start-timestamps for the last 90 days;
 - h. Details regarding whether or not the user's email address was verified by Discord;
 - i. Friends list for the user; and
 - j. Messages and attachments that users send to each other in text channels, whether in a server or in direct messages.
74. Therefore, the computers of Discord are likely to contain all the materials just described, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and account application.

Reddit

75. Reddit is a messaging platform owned by Reddit Inc. ("Reddit"), a company based in San Francisco, California. Reddit allows users to create their own accounts through which they can post public messages or send private messages to other users. Reddit also operates redditgifts.com and associated mobile applications.
76. Upon creating a Reddit account, a Reddit user must create a unique Reddit username and account password. While Reddit does not require users to provide their name and/or contact information, Reddit does and obtain maintain subscriber information, including name, address, identity information, billing information.
77. For each user, Reddit may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up.
78. Reddit also maintains IP logs for each user. These logs contain information about the user's logins to Reddit including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile. IP addresses, with the exception of the IP address used to create the account, are deleted after 100 days.
79. Reddit users post public messages on public bulletin boards, known as "subreddits". For example, people interested in discussing news regarding a specific item or reviews for vendors would post under the applicable subreddit. Subreddits are created by Reddit users and may be moderated by the creator of the subreddit and moderators to whom the user gives moderator status. Each subreddit may also have an associated wiki, a page for providing supplementary materials such as instructions, background, or recommended reading.

80. As discussed above, Reddit users can use their Reddit accounts to post public or send private messages. Each post or message includes a timestamp that displays when the message was posted to Reddit. Reddit users can also reply or comment to the posts of other users, or “upvote” the post to indicate their support for its contents.
81. In addition to posting publicly, Reddit users can send private messages to other Reddit users. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users.
82. Based on its online law enforcement guide, I know that Reddit maintains the following information for its accounts:
 - a. Subscriber information, including the username / subscriber identity, IP logs (including registration IP), the user’s name (if any), and the user’s email address (if any);
 - b. Other non-content records about the user or the user’s conduct on Reddit, including user preferences and communication headers;
 - c. Content of public communications, including posts, comments, and other information regarding the substance of a user’s public available communications; and
 - d. Content of non-public communications, including non-public messages / communications between the users; information about a user’s votes, posts, and comments; and other information regarding the substance of a user’s communications on non-public subreddits.
83. As explained herein, information stored in connection with a Reddit account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Reddit user’s account information, email address, IP log, stored electronic communications, and other data retained by Reddit, can indicate who has used or controlled the Reddit account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, public posts (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Reddit account at a relevant time. Further, Reddit account activity can show how and when the account was accessed or used. For example, as described herein, Reddit logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation.

Such information allows investigators to understand the geographic and chronological context of Reddit access, use, and events relating to the crime under investigation. Last, Reddit account activity may provide relevant insight into the Reddit account owner's state of mind as it relates to the offense under investigation. For example, information on the Reddit account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

84. In my training and experience, I know that Reddit uses small pieces of data sent from its website and stored in a user's web browser, called "cookies", to allow Reddit to record certain information about a user's visits to Reddit. This information would include the identity of particular computers that have logged in to Reddit. Using this information, Reddit can identify for law enforcement additional accounts that have been logged into from a particular computer. There is probable cause to believe that this information will lead to the discovery of additional evidence used in furtherance of the offenses being investigated.
85. Reddit can also identify other accounts linked to a particular account based on common telephone number; accounts used as a secondary, alternate, or recovery accounts; or a common machine cookie that may have been linked to an account within the last 30 days. Based on my training and experience, such information also constitutes evidence of the crimes under investigation where the information can be used to discover or confirm the identity of an online account's user or users at a particular time and to identify other accounts used by the same user.

Twitter

86. Twitter Inc. ("Twitter") is an electronic communications service and/or remote computing service provider headquartered at 1355 Market Street, Suite 900, San Francisco, California, 94103. Twitter owns and operates a social networking and microblogging service of the same name that can be accessed at <http://www.twitter.com> and via the Twitter mobile application ("app"). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.
87. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called "Tweets," with the public or, alternatively, to "protect" their Tweets by making them viewable by only a preapproved list of "followers." Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets ("retweet") or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.
88. Twitter also permits its users to exchange private messages, known as "direct messages" or "DMs," with other Twitter users. DMs, which also may include photos, videos, links,

and/or text, can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users. Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter user has the ability to alter the settings on their Twitter account so that they can receive direct messages only from (1) individuals to whom the user has already sent a direct message and (2) Twitter accounts that the user “follows” via his account.

89. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to “follow” accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter’s website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique user ID (“UID”). A user must also select a password as well as a unique Twitter username (also known as a “handle”). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the “display name”), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change their password, username, and/or display name at any time, but the UID for the account will remain constant.
90. While anyone can sign up and use Twitter for free, as of November 2021 Twitter also offered a subscription model that offered users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue at any time.
91. At the time of account creation, Twitter asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. Twitter also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user’s account was created; and (2) the method of account creation (e.g., website or Twitter app).
92. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information including (1) the user’s Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved “followers”). The user can personalize this page by posting a personal picture or image (known as an “avatar”) to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify his location, to provide a link to his website, or to specify his date of birth.
93. As noted above, Twitter users can use their account to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as

a “mention.” The Twitter user mentioned in the Tweet will receive a notification informing them that they have been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to their message, and the notification will show the content of that reply.

94. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts <http://t.co/>. Twitter tracks how many times these shortened links are clicked.
95. A registered Twitter user can also “like” a Tweet by clicking a heart icon on a Tweet sent by another user. If another user “likes” a Tweet that is posted by the Twitter user, a notification will appear in the user’s account identifying what Tweet was liked and who liked it.
96. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a “media timeline” on their profile that displays “the photos, videos, and GIF’s [the account holder] has uploaded with [their] Tweets.” An individual can view a Twitter user’s media timeline by visiting the user’s Twitter profile page.
97. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access their precise location information, the Twitter user will have the option of attaching their location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter’s in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user’s choice as well as the device’s precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing their location from their Tweets) at any time, and they can delete their past location data from Tweets that have already been sent.
98. A Twitter user may choose to “follow” another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the “follow” button on the other user’s Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the “follow” button and waiting for the other user to approve their request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user’s Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform them about the new follower. Each user’s Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can “unfollow” other users whom they previously followed at any time. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

99. A Twitter user can also “block” other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user’s Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks them.
100. A Twitter user can also use Twitter’s integrated search function. When a user types a search term into Twitter’s search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.
101. A Twitter user can also join or create “Lists” of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which it may appear.
102. Twitter also offers a functionality called “Spaces,” which it calls “a new way to have audio conversations on Twitter.” Any user can create a Space; that user is referred to as the “host.” Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to their Space and invite them to join. By default, the only individuals permitted to speak in a Space are the individuals that the host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can be in a Space at a given time.
103. Twitter also offers the ability to sign into third-party apps and websites using one’s Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using their Twitter account. Doing so grants the third-party service access to the Twitter user’s account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user’s Tweets, see who the user follows on Twitter, post Tweets to the user’s profile, or access the user’s email address. A user can revoke a third-party app or website’s authorization to access their Twitter account and associated data at any time.
104. Twitter collects and retains information about a user’s use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user’s Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user’s account; (4) the content uploaded to a user’s profile page, including their avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. Twitter also collects and retains various other data about a user and his/her activity, including:

- a. Logs of Internet Protocol (“IP”) addresses used to login to Twitter and the timestamp associated with such logins;
 - b. Transactional records reflecting, for example, when a user changed their display name or email address;
 - c. The identities of accounts that are blocked or muted by the user; and
 - d. Information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.
105. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter’s terms of service, during which time the Twitter user will be prevented from using Twitter’s services.
106. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other things, the browser being used, its version number, and details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user’s browser and operating system.
107. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.
108. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity involving child pornography offenses, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.
109. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Twitter can indicate who has used or controlled the account. This “user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

110. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).
111. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.
112. Therefore, Twitter’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the child pornography and child exploitation offenses under investigation including information that can be used to identify the account’s user or users.

Other Messenger Applications

113. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
114. The Kik messenger application is administered by MediaLab.ai Inc., a company based in Santa Monica, California. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
115. Unlike many other smartphone instant messenger applications that are based on a user’s telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik’s platform. Each user also creates a user profile, which includes a first and last name and an email address. MediaLab.ai Inc. does not verify this information, and as such, users can provide inaccurate information.

116. Telegram Messenger is a cloud-based instant messaging and voice over IP service that is owned by Telegram Messenger LLP, a privately-held international company. The application can be downloaded and used free of charge on smartphones, tablets, and computers. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. In addition, Telegram allows users to make voice calls to other users.
117. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chats on Telegram's servers. The secret chats provide users with the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires. Telegram also offers users the ability to lock their chats with a passcode. These locked chats cannot be viewed on the user's device without entering the passcode.
118. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize a number of social media and messenger accounts (including Instagram, Snapchat, and Telegram) to trade child pornography files and to discuss the sexual exploitation of children.

Collectors of Child Pornography

119. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce,

convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

NCMEC and CyberTipline Reports

- 120. The National Center for Missing and Exploited Children (commonly known as “NCMEC”) was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform a number of programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
- 121. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the CyberTipline reports. These ICAC’s

review the CyberTipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

FACTS SUPPORTING PROBABLE CAUSE

Background on MCGEORGE

122. MCGEORGE's date of birth is XX/XX/2000 (intentionally redacted for purposes of this Affidavit). He is presently 22 years old.
123. Records from the Ohio Bureau of Motor Vehicles identified that MCGEORGE currently utilizes the address of 111 West Cherry Street in New Paris, Ohio (hereinafter referred to as the "SUBJECT PREMISES") on his current Ohio driver's license. The investigation has determined that MCGEORGE resides at the SUBJECT PREMISES with his mother, Marty McGeorge, and his stepfather.

CyberTipline Reports

124. During the approximate time period of May 2022 through July 2022, approximately 33 reports were filed to NCMEC's CyberTipline regarding a total of approximately 201 suspected child pornography or child exploitation files that were located in various Discord, Reddit, Instagram, Kik, and Snapchat accounts. Further investigation revealed that IP addresses subscribed to an account at the SUBJECT PREMISES were utilized to access all of the accounts listed in the CyberTipline reports (as further detailed below). The reports provide information regarding the following accounts:
 - a. A Snapchat account containing the user name **dakingcobra69**;
 - b. Two Reddit accounts containing the user names of **KingCobraKai7** and **Outside-Difference66**;
 - c. Two Discord accounts containing the user names of **KingCobraKai69#6844** and **DatKingCobraKai420#4263**;
 - d. An Instagram account containing the user name **kinstonmcgeorge**; and
 - e. A Kik account containing the user name of **kingcobrakai69**.
125. NCMEC forwarded the approximately 33 CyberTipline reports and the accompanying files to the Cuyahoga County ICAC. Some of these reports were thereafter sent to the New Paris Police Department for further investigation. I have obtained and reviewed the approximately 33 CyberTipline reports and approximately 200 of the 201 accompanying

suspected child pornography or child exploitation files. Based on my review of the files and my training and experience, I believe that at least approximately 190 of the 200 files that I have reviewed (that being approximately 188 images and two videos) depict child pornography. The CyberTipline reports are detailed below in the following paragraphs.

Discord Inc. Reports – **KingCobraKai69#6844** Discord Account:

126. During the approximate time period of July 7, 2022 through August 13, 2022, Discord Inc. filed approximately nine reports to NCMEC's CyberTipline regarding a total of approximately 170 suspected child pornography or child exploitation files that were located in a Discord account containing a user name of **KingCobraKai69#6844** and a user identification number of **586587119187918849**. The report identified that the account was associated with the email address **kinstonmcgeorge69@gmail.com** and the telephone number 937-305-0680.
127. Discord Inc. reported that the approximately 170 suspected child pornography or child exploitation files were uploaded to the **KingCobraKai69#6844** Discord account during the approximate time period of May 29, 2022 through June 20, 2022. Discord Inc. further reported that the following IP addresses were utilized to upload the files: the IP address of 71.213.192.39, which was utilized to upload files associated with approximately three of the CyberTipline reports; the IP address of 71.213.197.217, which was utilized to upload files associated with approximately four of the CyberTipline reports; the IP address of 71.213.137.150, which was utilized to upload files associated with approximately two of the CyberTipline reports; and the IP address of 70.61.46.68, which was utilized to upload files associated with one of the CyberTipline reports.
128. I have reviewed the approximately 170 files that Discord Inc. reported in its CyberTipline reports. Based on my training and experience, I believe that at least approximately 165 of these files depict child pornography. By way of example, four of the files are described as follows:
 - a. IMG_20220531_032248_132.jpg: The file is an image that depicts what appears to be a nude prepubescent white female child who is lying on her stomach. What appears to be an adult white male is inserting his penis into the child's vagina, and what appears to be another adult white male is inserting his penis into the child's anus. The word "RAPE" is written on the child's left leg, and the words "PRINCESS" and "PRP 2016" are written on the child's right leg.
 - b. IMG_20220531_032337_556.jpg: The file is an image that depicts what appears to be a nude toddler-aged white female child who is lying on her back and covering her eyes with her hands. What appears to be an adult white male is inserting his penis into the child's anus.
 - c. IMG_20220531_032601_866.jpg: The file is an image that depicts what appears to

be an adult white male inserting his penis into the mouth of a prepubescent white female child who appears to be sleeping.

- d. IMG_20220531_032847_406.jpg: The file is an image that depicts what appears to be a prepubescent white female child who is wearing black stockings but is otherwise nude. The child is lying on her back, and her arms are over her head and bound together with a yellow rope. Her legs are bent and straddled, and each leg is bound with yellow ropes. Her nude vagina is exposed to the camera.
129. Lumen Technologies was identified as being the service provider for the IP address of 71.213.192.30. On or around July 7, 2022, an investigator from the Cuyahoga County ICAC served Lumen Technologies with an administrative subpoena requesting subscriber information for this IP address on one of the dates and times it was utilized to upload one of the child pornography files to the **DaKingCobraKai69#6844** Discord account. Records received from Lumen Technologies in response to the subpoena identified that this IP address was subscribed to Marty McGeorge (MCGEORGE's mother) at the SUBJECT PREMISES. The records further identified that this IP address was assigned to Marty McGeorge's account from approximately March 7, 2022 through June 6, 2022.
130. Lumen Technologies was also identified as being the service provider for the IP address of 71.213.197.217. On or around July 25, 2022, an investigator from the Cuyahoga County ICAC served Lumen Technologies with an administrative subpoena requesting subscriber information for this IP address on one of the dates and times it was utilized to upload one of the child pornography files to the **DaKingCobraKai69#6844** Discord account. Records received from Lumen Technologies in response to the subpoena identified that this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES. The records further identified that this IP address was assigned to Marty McGeorge's account from approximately June 7, 2022 through June 12, 2022.

Discord Inc. Report – **DaKingCobraKai420#4263** Discord Account:

131. On or around August 18, 2022, Discord Inc. filed approximately one report to NCMEC's CyberTipline regarding approximately two suspected child pornography or child exploitation files that were located in a Discord account containing a user name of **DaKingCobraKai420#4263** and a user identification number of **802267151120465970**. The report identified that the account was associated with the email address **kinstonmcgeorge6@gmail.com**.
132. Discord Inc. reported that the approximately two suspected child pornography or child exploitation files were uploaded to the **DaKingCobraKai4#4263** Discord account on or around July 11, 2022. Discord Inc. further reported that the IP address of 71.213.137.150 was utilized to upload these files.
 - a. The IP address of 71.213.137.150 that is listed in this report matches one of the IP

addresses utilized to access the **KingCobraKai69#6844** Discord account.

133. I have reviewed the approximately two files that Discord Inc. reported in its CyberTipline report. Based on my training and experience, I believe that both of the files depict child pornography. By way of example, one of the files is described as follows:
 - a. IMG_20220711_084948_668.jpg: The file is an image that depicts what appears to be two nude prepubescent white female children and a nude adult white male in a bathtub together. The adult male is inserting his penis into one child's mouth, and a substance that appears to be semen (which may be superimposed on the image) is on the child's mouth and chest. The other child is licking the apparent semen off of the first child's chest.
134. Lumen Technologies was identified as being the service provider for the IP address of 71.213.137.150. On or around August 19, 2022, an investigator from the Cuyahoga County ICAC served Lumen Technologies with an administrative subpoena requesting subscriber information for this IP address on one of the dates and times it was utilized to upload one of the child pornography files to the **DaKingCobraKai420#4263** Discord account. Records received from Lumen Technologies in response to the subpoena identified that this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES. The records further identified that this IP address was assigned to Marty McGeorge's account from approximately June 14, 2022 through July 11, 2022.

Reddit Inc. Reports – **KingCobraKai7** Reddit Account:

135. During the approximate time period of June 8, 2022 through July 27, 2022, Discord Inc. filed approximately 13 reports to NCMEC's CyberTipline regarding a total of approximately 13 suspected child pornography or child exploitation files that were located in a Reddit account containing a user name of **KingCobraKai7**. The report identified that the account was associated with the email address **kinstonmcgeorge80@gmail.com**.
136. Reddit Inc. reported that the approximately 13 suspected child pornography or child exploitation files were uploaded to the **KingCobraKai7** Reddit account during the approximate time period of May 19, 2022 through June 7, 2022. Reddit Inc. further reported that the following IP addresses were utilized to upload the files: 71.213.197.217, which was utilized to upload approximately 10 of the files, and 71.213.192.39, which was utilized to upload three of the files.
 - a. The IP address of 71.213.197.217 that is listed in this report matches one of the IP addresses utilized to access the **KingCobraKai69#6844** Discord account. As detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately June 7, 2022 through June 12, 2022.
 - b. The IP address of 71.213.192.39 that is listed in this report matches one of the IP

addresses utilized to access the **KingCobraKai69#6844** Discord account. As detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately March 7, 2022 through June 6, 2022.

137. I have reviewed the approximately 13 files that Reddit Inc. reported in its CyberTipline reports. Based on my training and experience, I believe that approximately 11 of these files depict child pornography. By way of example, three of the files are described as follows:
- a. gx84jsr0m7491.jpeg: The file is an image that depicts what appears to be a prepubescent white female child kneeling on her hands and knees on a bed. What appears to be a nude adult white male is kneeling behind the child and inserting his penis into the child's vagina or anus.
 - b. 7d2rn1s0m7491.jpeg: The file is an image that depicts what appears to be two nude toddler-aged white female children in a bathtub. One child ("Child 1") is kneeling on her hands and knees. The other child is using her hands to spread apart Child 1's buttocks, exposing Child 1's nude anus and vagina to the camera. What appears to be a white male (whose face and most of his body are not captured in the image) is using his hand to push Child 1's leg aside.
 - c. g7kyhyq3r2391.jpeg: The file is an image that depicts what appears to be a prepubescent white female child and a nude adult white male. The child is holding the adult male's penis with her hand and sticking out her tongue. A substance that appears to be semen is on the adult male's penis and the child's lip and tongue.

Reddit Inc. Reports – **Outside-Difference66** Reddit Account:

138. On or around July 11, 2022, Discord Inc. filed approximately seven reports to NCMEC's CyberTipline regarding a total of approximately seven suspected child pornography or child exploitation files that were located in a Reddit account containing a user name of **Outside-Difference66**. The report identified that the account was associated with the email address **kinstonmcgeorge6@gmail.com**.
- a. The email address of **kinstonmcgeorge6@gmail.com** that is listed in this report matches the email address that is associated with the **DaKingCobraKai420#4263** Discord account.
139. Reddit Inc. reported that the approximately seven suspected child pornography or child exploitation files were uploaded to the **Outside-Difference66** Reddit account on or around July 9, 2022 and July 10, 2022. Reddit Inc. further reported that the IP address of 71.213.137.150 was utilized to upload these files.
- a. The IP address of 71.213.137.150 that is listed in this report matches one of the IP addresses utilized to access the **KingCobraKai69#6844** and

DaKingCobraKai420#4263 Discord accounts. As detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately June 14, 2022 through July 11, 2022.

140. I have reviewed the approximately seven files that Reddit Inc. reported in its CyberTipline reports. Based on my training and experience, I believe that approximately six of these files depict child pornography. By way of example, three of the files are described as follows:
- a. aoul0rmztha91.jpeg: The file is an image that depicts what appears to be a nude pre-pubescent white female child and a nude adult white female in a bathtub together. The adult female is pushing the child's head onto her vagina, and it appears that the child is performing oral sex on the adult female.
 - b. klkzur5vnha91.jpeg: The file is an image that depicts what appears to be a nude prepubescent white female child lying on her back with her legs spread apart. It appears that the child is sleeping, and her nude vagina is exposed to the camera. A substance that appears to be semen is on the child's vagina and abdomen.
 - c. 85iiec5xtha91.jpeg: The file is an image that depicts what appears to be a prepubescent white female child who is wearing a pink hat but is otherwise nude. The child is kneeling on her hands and knees. What appears to be a nude adult white male is standing behind the child and inserting his penis into her anus.

Snap Inc. Report – **dakingcobra69** Snapchat Account:

141. On or around May 31, 2022, Snap Inc. filed a report to NCMEC's CyberTipline regarding approximately two suspected child pornography or child exploitation files that were located in a Snapchat account with the user name of **dakingcobra69**. The report identified that this Snapchat account was associated with the email address **kinstonmcgeorge80@gmail.com** and a telephone number of 937-305-0680. The report further identified that the Snapchat account user reported having a date of birth of XX/XX/2000.
- a. The email address of **kinstonmcgeorge80@gmail.com** that is listed in this report matches the email address that is associated with the **KingCobraKai7** Reddit account. The telephone number 937-305-0680 that is listed in this report matches the telephone number that is associated with the **KingCobraKai69#6844** Discord account.
 - b. The date of birth of XX/XX/2000 that is listed in this report matches MCGEORGE's date of birth.
142. Snap Inc. reported that the two suspected child pornography or child exploitation files were saved to, shared by, or uploaded to the **dakingcobra69** Snapchat account on or around May 30, 2022. Snap Inc. further reported that the IP address of 71.213.192.39 was utilized to log

into the Snapchat account on or around May 21, 2022.

- a. The IP address of 71.213.192.39 that is listed in this report matches one of the IP addresses utilized to access the **KingCobraKai69#6844** Discord account and the **KingCobraKai7** Reddit account. As detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately March 7, 2022 through June 6, 2022.
143. I have reviewed the approximately two files that Snap Inc. reported in its CyberTipline report. Based on my training and experience, I believe that at least one of these files depicts child pornography. This file is described as follows:
- a. dakingcobra69-None-7123b2d4-24c1-5ebf-98a7-145a2cda0598~5-d0db629394.mp4¹: The file is a video that depicts what appears to be a nude prepubescent white female child who is lying on her stomach on a blanket in an outdoor setting. What appears to be an adult white male states the following: “Suck my dick”. The child then gets up and performs fellatio on the adult male. The video is approximately 59 seconds in duration.

MediaLab.ai Inc. Report – kingcobrakai69 Kik Account:

144. On or around June 23, 2022, MediaLab.ai Inc. filed a report to NCMEC’s CyberTipline regarding approximately six suspected child pornography or child exploitation files that were located in a Kik account with the user name of kingcobrakai69. The report identified that this Kik account was associated with the email address **kinstonmcgeorge6@gmail.com**.
- a. The email address of **kinstonmcgeorge6@gmail.com** that is listed in this report matches the email address that is associated with the **DaKingCobraKai420#4263** Discord account and the **Outside-Difference66** Reddit account.
145. MediaLab.ai Inc. reported that the approximately six suspected child pornography or child exploitations files were sent by the kingcobrakai69 Kik account user to another user(s) via private chat messages on or around May 31, 2022. MediaLab.ai Inc. further reported that the IP address of 71.213.192.39 was utilized by the Kik account user when distributing these files.
- a. The IP address of 71.213.192.39 that is listed in this report matches one of the IP addresses utilized to access the **KingCobraKai69#6844** Discord account, the **KingCobraKai7** Reddit account, and the **dakingcobra69** Snapchat account. As

¹ When individuals send files via Snapchat to other users, the receivers typically see file names that are generated by the Snapchat application and not the file names as they appeared on the senders’ computers. Therefore, the file names noted in the CyberTipline reports and the file names of the files sent by Snap Inc. to NCMEC do not reflect the true file names.

detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately March 7, 2022 through June 6, 2022.

146. I have reviewed the approximately six files that MediaLab.ai Inc. reported in its CyberTipline report. Based on my training and experience, I believe that at least five of these files depict child pornography. By way of example, one of the files is described as follows:
- a. f4462972-4993-449f-a6fa-30280e4f9045.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child lying on a bed with her legs straddled. What appears to be an adult white male performs oral sex on the child. The video is approximately 19 seconds in duration.

Meta Platforms Inc. Report – **kinstonmcgeorge** Instagram Account:

147. On or around July 11, 2022, Meta Platforms Inc. filed a report to NCMEC's CyberTipline regarding one suspected child pornography or child exploitation file that was located in an Instagram account with the user name of **kinstonmcgeorge**, a user identification number of **54284524983**, and a profile name of KINSTON MCGEORGE. The report identified that this Instagram account was associated with the email address **kinstonmcgeorge80@gmail.com**. The report further identified that the Instagram account user reported having a date of birth of XX/XX/2000.
- a. The email address of **kinstonmcgeorge80@gmail.com** that is listed in this report matches the email address that is associated with the **KingCobraKai7** Reddit account and the **dakingcobra69** Snapchat account.
- b. The date of birth of XX/XX/2000 that is listed in this report matches MCGEORGE's date of birth.
148. Meta Platforms Inc. reported that the one suspected child pornography or child exploitation file was distributed by the **kinstonmcgeorge** Instagram account user to another user on or around July 10, 2022. Meta Platforms Inc. further reported that the IP address of 71.213.137.150 was utilized to log into the **kinstonmcgeorge** Instagram account on or around July 10, 2022.
- a. The IP address of 71.213.137.150 that is listed in this report matches one of the IP addresses utilized to access the **KingCobraKai69#6844** and **DaKingCobraKai420#4263** Discord accounts and the **Outside-Difference66** Reddit account. As detailed above, this IP address was subscribed to Marty McGeorge at the SUBJECT PREMISES from approximately June 14, 2022 through July 11, 2022.
149. As of the present time, I have not viewed the file that Meta Platforms Inc. submitted to

NCMEC as part of its CyberTipline report. However, I have noted the following additional information contained in the CyberTipline Report:

- a. Electronic Service Providers who submit files to NCMEC are requested, when feasible to do so, to categorize the content depicted in the files that they are reporting with the following designations:
 - i. Category A: a file depicting a suspected prepubescent minor,
 - ii. Category B: a file depicting a suspected pubescent minor,
 - iii. Category 1: a file depicting a “Sexual Act”, defined as being sexually explicit conduct, bestiality, masturbation, sadistic or masochistic abuse, or degradation,
 - iv. Category 2: a file depicting “Lascivious Exhibition”, defined as being nudity involving restraint, sexually suggestive poses, focus on genitalia, inappropriate touching, adult arousal, and/or spreading of limbs or genitals.
- b. As part of submitting the CyberTipline report, the Meta Platforms Inc. representative categorized the file that was distributed by the **kinstonmcgeorge** Instagram account user with the categories B1: depicting a suspected pubescent minor involved in a “Sexual Act”.
- c. An analyst from NCMEC compared the hash value of the file reported by Instagram Inc. in its CyberTipline report to a database containing files previously submitted to NCMEC by law enforcement officers, Electronic Service Providers, and other entities. Although the analyst did not view the file, the analyst noted that the file matched the hash value of another file(s) that was previously submitted to NCMEC and had been designated by an analyst(s) as depicting an apparent (but unconfirmed) child pornography.

Execution of Search Warrants

150. On or around July 26, 2022, search warrants were authorized by the Eaton (Ohio) Municipal Court authorizing the searches of the SUBJECT PREMISES and of MCGEORGE’s person and vehicle. Law enforcement officers from the New Paris Police Department and Preble County Sheriff’s Department executed these warrants on or around July 26, 2022.
151. MCGEORGE was contacted at his place of employment. He was observed accessing a cellular telephone, which he placed onto a table when officers approached him. This cellular telephone was thereafter seized, and it was identified as being a Samsung cellular telephone bearing a model number of SM-G781U. Various other electronic items were seized from the SUBJECT PREMISES pursuant to the warrant.

152. Officers conducted a brief interview of MCGEORGE after advising him of his Miranda rights. Below is a summary of some of the information provided by MCGEORGE during the interview:
- a. When asked what officers would find on his cellular telephone, MCGEORGE responded that he was “not sure”. He noted that he had “not done any searches in so long”.
 - b. MCGEORGE denied that he had recently searched for any type of pornography.
 - c. MCGEORGE advised that he had previously uploaded “memes and stuff” to his Reddit account. He denied having Twitter or Instagram accounts.
 - d. MCGEORGE acknowledged that the Samsung cellular telephone that officers had seized belonged to him, and he provided the passcode needed to access the device.

Examination of Samsung Cellular Telephone

153. On or around October 3, 2022, a search warrant was authorized by the Eaton Municipal Court authorizing the search of the Samsung cellular telephone and other electronic devices that were collected from MCGEORGE and the SUBJECT PREMISES on or around July 26, 2022. Some of the devices were thereafter submitted to the Ohio Attorney General’s Office, Bureau of Criminal Investigation, to be forensically examined.
154. Below is a summary of some of the information recovered during the forensic examination of the Samsung cellular telephone:
- a. Various artifacts were recovered that were indicative that MCGEORGE was the user of the device. Some of these artifacts include the following:
 - i. At least approximately 52 images and three videos depicting MCGEORGE were recovered from the device.
 - ii. Approximately four images depicting what appear to be work schedules with MCGEORGE’s name on them were recovered from the device.
 - iii. A number of chat messages were recovered from the device that were exchanged with others via various social media and messenger applications. In approximately two of the chats, the user of the device told other users the date of his birthday – and this date matches MCGEORGE’s birthday. In approximately three of the chats, others wished the user of the device a happy birthday – and the date of these chats again matched MCGEORGE’s birthday. In approximately six of the chats, the user of the device told others

that he was 21 years old. In approximately one of the chats, the user of the device told another individual that he lived in New Paris, Ohio.

- iv. As further detailed below, a number of user accounts for various social media and messenger applications were established on the device. Some of these user accounts (including Facebook, Telegram, and CashApp accounts) had profile names of KINSTON MCGEORGE.
- b. The following email accounts were established on the device:
kinstonmcgeorge45@gmail.com, **kinstonmcgeorge69@gmail.com** (the email address associated with the **KingCobraKai69#6844** Discord account and the **dakingcobra69** Snapchat account), **kinstonmcgeorge80@gmail.com** (the email address associated with the **KingCobraKai7** Reddit account, the **dakingcobra69** Snapchat account, and the **kinstonmcgeorge** Instagram account), **kinstonmcgeorge9000@gmail.com**, and **princesserianna96@gmail.com**². Email messages sent to and/or from these five accounts were recovered from the device. Among others, some of these email messages included the following:
 - i. Emails were received by the **kinstonmcgeorge45@gmail.com** account from an email address associated with Snap Inc. These email messages indicated that the **kinstonmcgeorge45@gmail.com** email account was associated with a Snapchat account with a user name of **kingcobraka2022**.
 - ii. Emails were received by the **kinstonmcgeorge6@gmail.com** account from email addresses associated with Twitter Inc., Snap Inc., and Discord Inc. These email messages indicated that the **kinstonmcgeorge6@gmail.com** account was associated with a Twitter account with a user name of **@KingCobraKai69**, a Snapchat account with a user name of **dakingcobrakai7**, and a Discord account with a user name of **DaKingCobraKai420** (which appears to be the same account listed in the CyberTipline report detailed above).
- c. A number of user accounts for various social media and messenger applications were established on the device. Some of these user accounts included the following:
 - i. Approximately 28 accounts associated with the email address **kinstonmcgeorge80@gmail.com** (the email address associated with the **KingCobraKai7** Reddit account, the **dakingcobra69** Snapchat account, and the **kinstonmcgeorge** Instagram account), including Google Photos and Google Drive accounts and a Facebook account with a profile name of KINSTON MCGEORGE;
 - ii. Approximately nine accounts associated with the email address

² Based on a preliminary review of this email account, it appears that it may be used by another individual.

kinstonmcgeorge6@gmail.com (the email address associated with the **DatKingCobraKai420#4263** Discord account, **Outside-Difference66** Reddit account, and **kingcobrakai69** Kik account), including a Google Drive account;

- iii. Approximately five accounts associated with the email address **kinstonmcgeorge9000@gmail.com**, including a Google Drive account;
- iv. Approximately 6 accounts associated with the email address **kinstonmcgeorge45@gmail.com**, including a Google Drive account;
- v. Approximately two accounts associated with the email address **kinstonmcgeorge7@gmail.com**, including a Google Drive account;
- vi. Approximately one user account associated with the email address **kinstonmcgeorge69@gmail.com** (the email address associated with the **KingCobraKai69#6844** Discord account and the **dakingcobra69** Snapchat account);
- vii. Approximately three user accounts associated with the email address **kinstonmcgeorge@yahoo.com**;
- viii. Approximately one user account associated with the email address **kinstonmcgeorge69@yahoo.com**;
- ix. Approximately one user account associated with the email address **kinstonmcgeorge80@yahoo.com**;
- x. A Twitter account with a user name of **kingcobrakai69**;
- xi. A Telegram account with a user identification number of 2106905346 and a profile name of KINSTON MCGEORGE;
- xii. Reddit accounts with user names of **Cultural_Yogurt_6309**, **Ok-Rooster5362**, **Fun_Management2465**, and **Prudent_Economy8810**;
- xiii. A Discord account with a user name of **DatKingCobraKai420#4263** (the account listed in the CyberTipline report detailed above);
- xiv. A CashApp account with a user name of KinstonMcGeorge, a profile name of KINSTON MCGEORGE, and a profile ID of C_n6d2khyrv; and
- xv. A Snapchat account with a user name of **kingcobraka2022**.

- d. At least approximately 2,151 images and 728 videos depicting child pornography were recovered from the device. These files include what appear to be some of the same images reported in the various CyberTipline reports detailed above. By way of example, seven of the files depicting child pornography are described as follows:
- i. 25633.jpg: The file is an image that depicts what appears to be a nude prepubescent white female child and an adult white male. There are purple straps binding the child's wrists to her ankles, a purple collar around her neck, and a purple covering over her eyes. The adult white male is kneeling in front of the child and having vaginal sexual intercourse with her.
 - ii. 8b9ViagC.jpg: The file is an image that depicts what appears to be a nude toddler-aged white female child lying on her stomach. What appears to be an adult white male is standing behind the child and inserting his penis into her vagina.
 - iii. Gk8Xia4b_1.jpg: The file is a close-up image of the nude vagina and abdomen of what appears to be a prepubescent white female child. What appears to be an adult white male's penis is inserted into the child's vagina. The word "Rape" is written on the child's abdomen.
 - iv. 1_5033115463710671431.3gb: The file is a video that depicts what appears to be a white female infant lying on her back. The infant is wearing a shirt but no pants. What appears to be an adult white female licks the infant's vagina. The video is approximately 21 seconds in duration.
 - v. 0LES1JJJ.jpg: The file is an image that depicts what appears to be a nude or partially nude white female child performing oral sex on a dog.
 - vi. 4yo LISA Fuck-and-Cum-in-Pussy.mp4: The file is a video that depicts what appears to be a nude prepubescent white female child lying on her back with her legs spread apart. What appears to be an adult white male has vaginal sexual intercourse with the child and then secretes what appears to be semen onto the child's vagina and anus. The video is approximately two minutes and 31 seconds in duration.
 - vii. Screen Recording 20220620-232559 Snapchat.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child and a nude adult white male. The adult male pushes the child's head onto his penis and inserts his penis into the child's mouth. The video is approximately nine seconds in duration.
- e. In addition to the child pornography files, thousands of images and videos were recovered from the device depicting children displaying states of nudity, child

erotica, possible child pornography (i.e., age questionable files), and animated or computer-generated child pornography.

- f. The Telegram application was installed on the device. Approximately 54 chats were recovered from the device that were exchanged between the Telegram account with the user identification number of 2106905346 and a profile name of KINSTON MCGEORGE (the account noted above) and other Telegram users during the approximate time period of March 2019 through July 2022. Below is a summary of some of the information contained in these Telegram chats:
 - i. The KINSTON MCGEORGE Telegram account user exchanged image and/or video files with a number of other users. Based on how the files were exchanged, a number of files were not recovered during the forensic extraction. Based on my review of the files that were properly extracted and my training and experience, I believe that more than 1,300 child pornography files were exchanged in at least 34 of the Telegram chats. More than 1,200 of the child pornography files were distributed by the KINSTON MCGEORGE Telegram account user in approximately 32 of the 34 chats. More than 150 of the child pornography files were received by the KINSTON MCGEORGE Telegram account user in approximately 13 of the 34 chats. In addition to the child pornography files, hundreds of files depicting children displaying states of nudity, child erotica, possible child pornography (i.e., age questionable files), and animated or computer-generated child pornography were also exchanged in the chats.
 - ii. Below are examples of a few of the chats in which the KINSTON MCGEORGE Telegram account user distributed and/or received child pornography files:
 1. On or around June 7, 2022, another user stated the following: “i have illegal”. The KINSTON MCGEORGE Telegram account user responded with the following: “Ok 🐼 send what ya got,”. The other user then sent three videos depicting child pornography. By way of example, one of the files had a file name of *1_5129876339540623760.mp4*. The file is a video that depicts what appears to be a prepubescent Asian or Hispanic female child performing fellatio on an adult male. The adult male then masturbates his penis. The video is approximately 45 seconds in duration. After the three video files were sent, the other user stated the following: “i have more”, “what u got”. The KINSTON MCGEORGE Telegram account user responded with the following: “Fuck bro, that so hot hell yeah”. The two users then exchanged a number of child pornography files.

2. On or around June 9, 2022, the KINSTON MCGEORGE Telegram account user sent another user a number of files, including images and videos depicting child pornography. By way of example, one of the files that the KINSTON MCGEORGE Telegram account user distributed had a file name of *1_4976528466426986942.mp4*. The file is a video that depicts what appears to be a toddler-aged Asian female child wearing a pink shirt but no pants or underwear. The child is lying on her back with her legs spread apart. What appears to be an adult white male has anal sexual intercourse with the child. The video is approximately 14 seconds in duration. After these files were sent, the other user stated the following: “Okayyy wawwww” . . . “I’m gonna have the best hanjdob of my life with this cp”. The KINSTON MCGEORGE Telegram account user responded with the following: “Awesome glad to help”.

3. On or around July 10, 2022, another user stated the following: “Just start sending and I’ll send as many as you send”. The KINSTON MCGEORGE Telegram account user responded with the following: “Don’t say that...”, “Don’t say that☺ I will challenge that”, “I have so much to just blow up this chat☺ also sometimes cuz I got shitty internet the more I send the longer it to send it all”, “Getting into a game with a buddy”. The other user then stated the following: “I have quite a bit I think I can keep up with the amount u send”. The KINSTON MCGEORGE Telegram account user stated the following: “Aight will see imma try an send after game”. The two users then exchanged a number of files, including child pornography files. By way of example, one of the files that the KINSTON MCGEORGE Telegram account user distributed had a file name of - *5066992740268616256_120.jpg*. The file is an image that depicts what appears to be a toddler-aged white female child who is wearing a shirt but no pants or underwear. The child is lying on her back with her legs spread apart, exposing her nude vagina. A substance that is consistent with semen in on the child’s vagina.

- iii. During some of the chats in which child pornography files were exchanged, the KINSTON MCGEORGE Telegram account user and/or the other users made comments indicating that they had met each other on the Reddit website.

- iv. In approximately four of the chats, the KINSTON MCGEORGE Telegram account user made comments indicating that he was an administrator for a Discord server. The KINSTON MCGEORGE Telegram account user told the other users that they could pay money to obtain child pornography and

“loli”³ files. Below are a few examples of some of these chats:

1. On or around June 8, 2022, the KINSTON MCGEORGE Telegram account user stated the following to another user: "There ya are mate all im able to do rn but ay im in a discord server where you can get access to cp for 5\$ im a mod". The other user responded with the following: "I don't have the money to do that I wish I did", "How do you pay to join", "I have the money to pay for it I just need to know how". The KINSTON MCGEORGE Telegram account user stated the following: "Talk to Kenpachi Goat and let him know", "That's his cashapp info but also does have paypal too". The KINSTON MCGEORGE Telegram account user then sent the other user screenshots of a Discord account with the user name of Kenpachi Goat (*with a goat emoji*) #5699 and a CashApp account with a user name of \$NightRaid18 and a profile name of Rimuru Tempest.
2. On or around July 6, 2022, the KINSTON MCGEORGE Telegram account user stated the following to another user: "Ayo wanna be in a discord server that with 5\$ ya can get into NLR (no limit raider) and get cp beastly and if ya into it even gore". The other user responded with the following: "Maybe, it depends really", "I'd need a sample here first", "And would it be through PayPal?". The KINSTON MCGEORGE Telegram account user responded with the following: "What ya mean sample? Amd idk let me check I think he's got cash app but I'll check" . . . "And yes he has paypal too".
3. On or around July 16, 2022, the KINSTON MCGEORGE Telegram account user stated the following to another user: "Cuz am a mod for a server that ewith 5\$ you can get into NL and see cp beastiality and without paying able to access loli", "Ofcourse other porn and hentia aswell" . . . "<https://discord.gg/KXFE5599>", "Yeah I can also give you the admins username to dm him to get into NL if you want".
- v. In one of the chats, the KINSTON MCGEORGE Telegram account user indicated that he knew people on Snapchat who were selling child pornography. Specifically, the KINSTON MCGEORGE Telegram account user stated the following: "Damn, I also got some ppl on snap that selling cp and thinking bout it, so if I do ill let ya know, and so let me know if you do that and how it goes aight".

³ “Lolita”, sometimes shortened to “loli”, is often used as a term to refer to a young girl or a young-looking girl. In animated or anime pornography, “loli” often refers to a female with a child-like appearance, regardless of whether or not she is under the age of 18 years old. Based on my training and experience, I know that “loli” is a term that is commonly used by offenders when searching for child pornography files and that is found in the names of child pornography files.

- vi. In approximately seven of the chats, the KINSTON MCGEORGE Telegram account user made comments about being recently "banned" or "locked out" of his Kik, Reddit, Discord, and/or Snapchat accounts. In one of the chats, which transpired on or around July 22, 2022, the KINSTON MCGEORGE Telegram account user indicated that he was having trouble finding individuals with whom to trade child pornography files because his Discord and Redddit accounts had been closed. Specifically, the KINSTON MCGEORGE Telegram account user stated the following: "Just trading as I do... well im kinda fucked on trading with my reddit and discords being banned and reddit changed there shit with a subreddit so no way of finding ppl into cp to trade with now but I am in a discord server right before reddit killed my account and you can access loli and CP tho fpr access to cp it 5\$ and im a mod of the NL raiders lol".
1. Based on my training and experience, I know that many Electronic Service Providers (including MediaLab.ai Inc., Reddit Inc., Discord Inc., and Snap Inc.) typically close users' accounts after finding child pornography files and submitting CyberTipline reports.
- vii. The KINSTON MCGEORGE Telegram account user made comments in some of the chats about having a lot of child pornography files. Below are examples of some of these comments:
1. On or around June 9, 2022, the KINSTON MCGEORGE Telegram account user sent a number of child pornography files to another user. Prior to sending the files, the KINSTON MCGEORGE Telegram account user stated the following: "Ah that's fine imm just bout bomb you increase ya collection". After sending the child pornography files, the KINSTON MCGEORGE Telegram account user stated the following: "Yeah, hope ya liked that fukin cp nuke☺☺".
2. On or around June 16, 2022, the KINSTON MCGEORGE Telegram account user stated the following to another user: "Ayo btw I got so much more cp to be able to trade ifnya want".
3. On or around June 22, 2022, the KINSTON MCGEORGE Telegram account user stated the following to another user: "Oh sup sorry was at work off now, bruh if ya came to trade I fukin got you manI was sent a big mega⁴ link, and fuck not to mentio it's been so long I got

⁴ Mega is an encrypted cloud storage service administered by Mega LTD, a company based in New Zealand. Based on my training and experience, I know that individuals involved in child pornography offenses often trade files by sending sharing links to their cloud storage accounts.

alot before that mega link, tho now I can't even trade cuz my 1st discord and my reddits were banned" . . . "But cuz of the mega link im in no need to trade im still looking through and was sent it bout a month or so ago".

4. On or around July 7, 2022, another user asked the following of the KINSTON MCGEORGE Telegram account user: "Can you send me the stuff". The KINSTON MCGEORGE Telegram account user responded with the following: "Ya have to think I talknto countless ppl in a day, get lotta stuff I can't always remember what I've gotten & sent lol im in a game rn".
- g. The Snapchat application was installed on the device. A total of approximately 73 chat messages were recovered from on the device that were exchanged via the Snapchat account with the user identification number of **a325813c-31ac-4553-897e-7d3ca0c2f4b0**, dated during the approximate time period of June 2022 through July 2022. The user of this Snapchat account made comments in two of the chats that were indicative that he was soliciting child pornography files. These comments are as follows:
 - i. On or around June 22, 2022, the Snapchat account user stated the following to another user: "Hello? You sell cp?".
 - ii. On or around June 25, 2022, the Snapchat account user stated the following to another user: "Cp menu?".
 - h. The Reddit application was installed on the device. Approximately 562 Reddit postings were recovered from the device that were made by various different Reddit users. Consistent with the comments made in some of the Telegram chats, a number of the Reddit postings were indicative that the users were attempting to find other users with whom to trade files – including child pornography files. By way of example, some of these postings include the following:
 - i. On or around June 7, 2022, a Reddit user stated the following: "send me legal or illegal nudes".
 - ii. On or around June 8, 2022, a Reddit user stated the following: "s2r⁵ cp girls".
 - iii. On or around March 27, 2022, a Reddit user stated the following: "Love

⁵ Based on my training and experience, I know that "S2R" is a term to refer to "Send to Receive". Individuals involved in child pornography offenses often utilize this term when communicating with other offenders. Such individuals use this term to instruct the other individuals that they must send child pornography before they can receive child pornography.

young cock”.

Conclusion Regarding Accounts

155. Based on all of the information detailed above, there is probable cause to believe that MCGEORGE is the user of the following:
- a. The Yahoo email accounts **kinstonmcgeorge@yahoo.com**, **kinstonmcgeorge69@yahoo.com**, and **kinstonmcgeorge80@yahoo.com**;
 - b. The Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com**, **kinstonmcgeorge6@gmail.com**, **kinstonmcgeorge80@gmail.com**, **kinstonmcgeorge45@gmail.com**, **kinstonmcgeorge9000@gmail.com**, and **kinstonmcgeorge7@gmail.com**;
 - c. The Snapchat accounts containing the user names **dakingcobra69**, **kingcobraka2022**, and **dakingcobrakai7** and the user identification number of **a325813c-31ac-4553-897e-7d3ca0c2f4b0**;
 - d. The Reddit accounts containing the user names **KingCobraKai7**, **Outside-Difference66**, **Cultural_Yogurt_6309**, **Ok-Rooster5362**, **Fun_Management2465**, and **Prudent_Economy8810**;
 - e. The Discord accounts containing the user names **KingCobraKai69#6844** and **DatKingCobraKai420#4263** and the user identification numbers **586587119187918849** and **802267151120465970**;
 - f. The Instagram account containing the user name **kinstonmcgeorge** and the user identification number **54284524983**;
 - g. The Kik account containing the user name **kingcobrakai69**;
 - h. The Twitter account containing the user name **@KingCobraKai69**;
 - i. The Samsung cellular telephone seized from MCGEORGE on or around July 26, 2022; and
 - j. The KINSTON MCGEORGE Telegram account that was contained on the above noted Samsung cellular telephone.
156. Also based on the information detailed in the Affidavit, there is probable cause to believe the following:

- a. MCGEORGE utilized at least one Snapchat account (the account with the user name of **dakingcobra69**), at least two Reddit accounts (the accounts with the user names of **KingCobraKai7** and **Outside-Differnce66**), at least two Discord accounts (the user names of **KingCobraKai69#6844** and **DatKingCobraKai420#4263**), at least one Instagram account (the account with the user name of **kinstonmcgeorge**), at least one Kik account (the account with the user name of **kingcobrakai69**), and at least one Telegram account (the account with the profile name of **KINSTON MCGEORGE**) to possess, receive, and distribute child pornography files.
 - b. MCGEORGE has utilized his Samsung cellular telephone to access his various social media and messenger accounts and to possess, receive, and distribute child pornography files.
 - c. MCGEORGE has utilized at least three email accounts (that being **kinstonmcgeorge69@gmail.com**, **kinstonmcgeorge6@gmail.com**, and **kinstonmcgeorge80@gmail.com**) to register some of the previously noted Snapchat, Reddit, Discord, Instagram, and Kik accounts. These email accounts therefore served as instrumentalities of MCGEORGE's child pornography offenses.
157. Based on my training and experience, I know that Samsung cellular telephones are manufactured outside the state of Ohio. I also know that accessing Snapchat, Reddit, Discord, Instagram, Kik, Twitter, and Telegram accounts require the user of the Internet and thereby affect Interstate or foreign commerce.

Evidence Available in Email and Social Media Accounts

158. In my experience, individuals often post information on their social media accounts about other electronic accounts that they utilize – including their email addresses, other social media accounts, and messenger accounts. This information may provide evidentiary value to child exploitation investigations in that they help in identifying other accounts utilized by the offenders in furtherance of their child exploitation activities.
159. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
160. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to

communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

161. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
162. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.
163. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
164. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.
165. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases

where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

166. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

167. As detailed above, there is probable cause to believe that MCGEORGE utilizes Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com**, **kinstonmcgeorge6@gmail.com**, **kinstonmcgeorge80@gmail.com**, **kinstonmcgeorge45@gmail.com**, **kinstonmcgeorge9000@gmail.com**, and **kinstonmcgeorge7@gmail.com**.
168. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.
169. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
170. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.
171. Based on my training and experience, I know that location information from cellular telephones and Google accounts can be materially relevant in investigations involving child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.

Conclusion Regarding Probable Cause

172. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts may contain evidence of MCGEORGE's child pornography offenses:
- a. The Yahoo email accounts **kinstonmcgeorge@yahoo.com**, **kinstonmcgeorge69@yahoo.com**, and **kinstonmcgeorge80@yahoo.com**;
 - b. The Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com**, **kinstonmcgeorge6@gmail.com**, **kinstonmcgeorge80@gmail.com**, **kinstonmcgeorge45@gmail.com**, **kinstonmcgeorge9000@gmail.com**, and **kinstonmcgeorge7@gmail.com**;
 - c. The Snapchat accounts containing the user names **dakingcobra69**, **kingcobraka2022**, and **dakingcobrakai7** and the user identification number of **a325813c-31ac-4553-897e-7d3ca0c2f4b0**;
 - d. The Reddit accounts containing the user names **KingCobraKai7**, **Outside-Difference66**, **Cultural_Yogurt_6309**, **Ok-Rooster5362**, **Fun_Management2465**, and **Prudent_Economy8810**;
 - e. The Discord accounts containing the user names **KingCobraKai69#6844** and **DatKingCobraKai420#4263** and the user identification numbers **586587119187918849** and **802267151120465970**;
 - f. The Instagram account containing the user name **kinstonmcgeorge** and the user identification number **54284524983**; and
 - g. The Twitter account containing the user name **@KingCobraKai69**
173. Preservation requests were served to Yahoo Inc., Google LLC, Snap Inc., Reddit Inc., Discord Inc., Meta Platforms Inc., and Twitter Inc. for the above noted accounts. An investigator attempted to serve MediaLab.ai Interactive Inc. with a preservation request for the Kik account with the user name of kingcobrakai69 (the account listed in the CyberTipline report detailed above). However, MediaLab.ai Inc. responded to the request by stating that the company had already purged all data associated with this account.

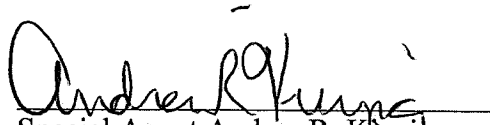
ELECTRONIC COMMUNICATIONS PRIVACY ACT

174. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Yahoo Inc., Google LLC, Snap Inc., Reddit

Inc., Discord Inc., Meta Platforms Inc., and Twitter Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-7. Upon receipt of the information described in Section I of Attachments B-1 through B-7, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-7.

CONCLUSION

175. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 through A-7, including the following offenses: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1).
176. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-7.
177. Because the warrants for the accounts described in Attachments A-1 through A-7 will be served on Yahoo Inc., Google LLC, Snap Inc., Reddit Inc., Discord Inc., Meta Platforms Inc., and Twitter Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 9th of November 2022


Peter B. Silvain, Jr.
United States Magistrate Judge

 JUDGE

ATTACHMENT A-1
Property to Be Searched

Information associated with the email accounts **kinstonmcgeorge@yahoo.com**, **kinstonmcgeorge69@yahoo.com**, and **kinstonmcgeorge80@yahoo.com** that is stored at premises controlled by Yahoo Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California, 94089.

ATTACHMENT B-1
Particular Things to be Seized

I. Information to be disclosed by Yahoo Inc. (the “Provider”)

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1 for the time period of January 1, 2021 to the present:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service utilized;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-2
Property to Be Searched

Information associated with the Google accounts associated with the email addresses **kinstonmcgeorge69@gmail.com, kinstonmcgeorge6@gmail.com, kinstonmcgeorge80@gmail.com, kinstonmcgeorge45@gmail.com, kinstonmcgeorge9000@gmail.com, and kinstonmcgeorge7@gmail.com** that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B-2
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2 for the time period of January 1, 2021 to the present:

1. Subscriber Information: Any available subscriber information for the account, including the following: user-provided name; account email address; account status; Google services used by account; recovery email and SMS recovery number; account creation date and time; terms of service IP address, date, and time; language; Google Account ID ; last logins to the account, including IP address, date, and time; and accounts associated with a particular device, SMS recovery number, IMEI, or Android ID.
2. IP Logs: Logs of IP addresses utilized to access the Google account.
3. Gmail: The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.
4. Contacts: Any records pertaining to the user’s contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.
5. Calendar: Any records pertaining to the user’s calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history.
6. Messaging: The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
7. Google Drive and Google Keep: The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data

and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

8. Photos: The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
9. Maps: All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.
10. Location History: All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
11. Chrome and My Activity: All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Cloy Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any Internet or search history indicative of searching for child pornography or content involving children.
5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
6. Any communications with minors, and any identifying information for these minors.
7. Any information related to the use of aliases.
8. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
9. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
10. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
11. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
12. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-3
Property to Be Searched

Information associated with the Snapchat accounts containing the user names **dakingcobra69**, **kingcobraka2022**, and **dakingcobrakai7** and the user identification number of **a325813c-31ac-4553-897e-7d3ca0c2f4b0** that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company that accepts service of legal process at 2772 Donald Douglas Loop North, Santa Monica, California, 90405.

ATTACHMENT B-3
Particular Things to be Seized

I. Information to be disclosed by Snap Inc. (the “Provider”)

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-3 for the time period of January 1, 2021 to the present:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents for previous snaps, stories, and Chats, to include any metadata and/or content;
- (c) Content of sent snaps, story content, and chat content;
- (d) Contents of user’s Memories, Snapchat’s cloud-storage service;
- (e) All Logs (including sender, recipient, date, and time) concerning the previous Snaps sent to or from the Snapchat account of the listed account, to include IP addresses associated with the account;
- (f) The types of service utilized by the user;
- (g) The length of service (including start date) and the means and source of any payments associated with the service (including debit card or bank account numbers);
- (h) All privacy settings and other account settings, including privacy settings for individual Snaps, and all records showing which Snapchat users have been blocked by the account;
- (i) All records pertaining to communications between the Provider and any person regarding the user or the user’s account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Cloy Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-4
Property to Be Searched

Information associated with the Reddit accounts containing the user names KingCobraKai7, Outside-Difference66, Cultural_Yogurt_6309, Ok-Rooster5362, Fun_Management2465, and Prudent_Economy8810 that is stored at premises owned, maintained, controlled, or operated by Reddit Inc., a company that is headquartered at 548 Market Street # 16093, San Francisco, California, 94104. The company accepts service of legal process via care of Corporation Service Company, 2710 Gateway Oaks Drive, Suite 160N, Sacramento, California, 95833.

ATTACHMENT B-4
Particular Things to be Seized

I. Information to be disclosed by Reddit Inc. (the “Provider”)

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-4 for the time period of January 1, 2021 to the present:

- a. Subscriber information, including the username / subscriber identity, IP logs (including registration IP), the user’s name (if any), and the user’s email address (if any);
- b. Other non-content records about the user or the user’s conduct on Reddit, including user preferences and communication headers;
- c. Content of public communications, including posts, comments, and other information regarding the substance of a user’s public available communications;
- d. Content of non-public communications, including non-public messages / communications between the users; information about a user’s votes, posts, and comments; and other information regarding the substance of a user’s communications on non-public subreddits;
- e. Other accounts linked to the accounts listed in Attachment A-4 by cookies; telephone number; or secondary, alternate, or recovery accounts;
- f. All records pertaining to communications between the Provider and any person regarding the user or the user’s accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clys Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-5
Property to Be Searched

Information associated with the Discord accounts containing the user names KingCobraKai69#6844 and DatKingCobraKai420#4263 and the user identification numbers 586587119187918849 and 802267151120465970 that is stored at premises owned, maintained, controlled, or operated by Discord Inc., a company that accepts service of legal process at 444 De Haro Street, Suite 200, San Francisco, California, 94107.

ATTACHMENT B-5
Particular Things to be Seized

I. Information to be disclosed by Discord Inc. (the “Provider”)

To the extent that the information described in Attachment A-5 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-5 for the time period of January 1, 2021 to the present:

- a. The unique user ID number of the account that is assigned by Discord;
- b. Registration date and time for the account;
- c. Registration IP address of the account;
- d. Email address provided by the user;
- e. User’s current username and tag number;
- f. Billing information for paid subscribers;
- g. IP addresses and session start-timestamps for the last 90 days;
- h. Details regarding whether or not the user’s email address was verified by Discord;
- i. Friends list for the user; and
- j. Messages and attachments that users send to each other in text channels, whether in a server or in direct messages.
- k. All records pertaining to communications between the Provider and any person regarding the user or the user’s accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clys Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-6
Property to Be Searched

Information associated with the Instagram account containing user name **kinstonmcgeorge** and the user identification number **54284524983** that is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc., a company that accepts service of legal process at 1601 Willow Road, Menlo Park, California, 94025.

ATTACHMENT B-6

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms Inc. (the “Provider”)

To the extent that the information described in Attachment A-6 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-6 for the time period of January 1, 2021 to the present:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;
- e. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;
- f. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- g. All communications or other messages sent or received by the account;
- h. All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;
- i. All photographs and images in the user gallery for the account;
- j. All location data associated with the account, including geotags;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list), as well as any friends of the user;

- m. A list of all users that the account has “unfollowed” or blocked;
- n. All privacy and account settings;
- o. All records of Instagram searches performed by the account, including all past searches saved by the account;
- p. All information about connections between the account and third-party websites and applications; and,
- q. All records pertaining to communications between the Provider and any person regarding the user or the user’s Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clys Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT A-7
Property to Be Searched

Information associated with the Twitter account containing the user name **@KingCobraKai69** that is stored at premises owned, maintained, controlled, or operated by Twitter Inc., company that accepts service of legal process at 1355 Market Street, Suite 900, San Francisco, California, 94103.

ATTACHMENT B-7
Particular Things to be Seized

I. Information to be disclosed by Twitter Inc. (the “Provider”):

To the extent that the information described in Attachment A-7 is within the possession, custody, or control of Twitter, regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to Twitter, Twitter is required to disclose to the government for each account or identifier listed in Attachment A-7 for the time period of January 1, 2021 to the present:

- A. All business records and subscriber information, in any form kept, pertaining to the Account, including:
 - 1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;
 - 2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);
 - 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 - 4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 - 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 - 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers, [[from January 1, 2006 to the present;
 - 7. Privacy and account settings, including change history; and
 - 8. Communications between Twitter and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content, records, and other information relating to communications sent from or received by the Account from January 1, 2006 to the present, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the Account, and all associated multimedia, metadata, and logs;
 2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the Account, including all attachments, multimedia, header information, metadata, and logs;
- C. All other content, records, and other information relating to all other interactions between the Account and other Twitter users from January 1, 2006 to the present, including but not limited to:
1. All users the Account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the Account;
 2. All information from the "Connect" or "Notifications" tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., "mentions" or "replies");
 3. All contacts and related sync information; and
 4. All associated logs and metadata;
- D. All other content, records, and other information relating to the use of the Account, including but not limited to:
1. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;
 2. All multimedia uploaded to, or otherwise associated with, the Account;
 3. All records of searches performed by the Account from January 1, 2006 to the present;
 4. All location information, including all location data collected by any plugins, widgets, or the "Tweet With Location" service, from January 1, 2006 to the present; and
 5. All information about the Account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the Account was clicked.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clys Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.